Over the past year, I have listened to my fellow engineers at Honeywell Commercial Electronic Systems (formerly Honeywell Commercial Aviation Products) regarding the use of cell phones on commercial aircraft, and have conducted preliminary hazard analysis for our air data and inertial navigation systems. As system safety and reliability engineer for all of our products, I am responsible for identifying hazards, conducting failure modes effects and criticality analysis, and making recommendations for mitigating actions. The Radio Technical Commission for Aeronautics and the Federal Aviation Administration have never approached me since I have been working at Honeywell regarding the potential use of cell phones onboard aircraft in flight, and these organizations have proceeded to analyze and make recommendations without our input to this issue. Honeywell Commercial Electronic Systems designs, builds, and tests air data and inertial navigation systems for most commercial airliners. These systems tell the pilot where the aircraft is, how fast the aircraft is moving, the attitude of the aircraft, and more. The systems we build are safety-critical. They are also vulnerable to outside interference from various sources. I will outline, what we believe to be hazards regarding the system as well as how normal and abnormal cell phone usage would contribute to an adverse event. I will explain why airlines should not proceed too hastily with allowing cell phones on aircraft and what would have to be done to ensure safe use with our systems.

The hazards onboard an aircraft concerning an Air Data Inertial Reference Unit (ADIRU) can be described as one high-level hazard. We define a hazard an event that is prerequisite to a mishap. Erroneous air data and/or navigation information results in equipment damage and/or personnel injury or death or complete loss of a system when coupled with other events, and we determine the probability of these events. We can define interference from radio frequency sources such as cell phones as an event that is prerequisite to this mishap. A sequence of events, sometimes described with a condition-event sequence description or with a fault tree, demonstrates how a failure or another event contributes to the probability of a mishap. Honeywell has mapped almost every conceivable failure mode based upon distinct types of outputs to the aircraft system. These failure modes include incorrect airspeed, altitude, attitude, position, and external temperature and so on. This information is measured by three ring laser gyros, three accelerometers, and data probes on an aircraft. Our box will process this information and provide it to the system that displays it to the pilot or even directly into feedback to an engine and/or other flight controls and for crew display. Data can be transmitted either analog or digitally to and from sensors and to and from the higher-level system (the aircraft) or both. Adequate shielding from radio frequency radiation is not always achieved whether among these systems or even within a box such as the ADIRU itself simply because either it was never required or not seen as needed. It is true that requirements-based engineering is new and older systems were based on much looser requirements than today's well-defined requirements. These systems are still flying today. It is important to note that many Honeywell navigation systems are more than 25 years old, and none were required to be tolerant to cell phone interference. These systems were never tested to be safe from cell phone interference on every aircraft type. Each navigation system-aircraft type

combination will have unique properties as will most cell phones and
cell phone failure modes.

What is required now is that a fleet of aircraft subsystems will
perform to a specified mean time between failures (MTBF) over the
lifespan of an aircraft. Some aircraft have lives of more than 50
years, and I expect that some of the navigation subsystems will be
flying on these aircraft for just as long.

Processors and their interfaces use signals transmitted at high
frequencies. As time goes by, demand for faster processors ensure
that radio frequency radiation is more and more likely to interfere
with data transmissions regardless of spread spectrum technological
improvements made. Such is the concern for the avionics industry.
This is also especially a concern for the military. While such
signals are protected from eavesdropping and jamming, this does not
necessarily mean that such signals do not interfere with digital
data. If not, then there would be no reason to provide shielding on
feed lines on low power military SINCGARS radio systems. The fact
is that while it is nearly impossible for enemy direction finding
equipment to find a transmitter using the same technology used on
cell phones, this does not preclude interference with other
subsystems near a transmitter.

The aerospace industry does not have an adequate standard to design,
build, or test avionics subsystems to be save from RF radiation from
cell phones. Right now, the RTCA only covers systems that are
installed on the aircraft. Furthermore, the RTCA has not involved
system safety engineers at Honeywell Commercial Aviation Products in
their discussions. This is not acceptable.

I expect aircraft subsystems to receive interference from cell
phones based upon years of experience of measuring signal strength
of low-power (1-3 Watt) transmitters inside aircraft. I also
believe that the number of cell phones (800 or more on A380) on some
aircraft will cause interference with safety-critical systems. I
also believe that each aircraft will have its own susceptibility
based on many factors that need to be explored such as fuselage
geometry and material, shielding of wires, and cell
phone/transmitter location to equipment. I also believe that we
must consider cell phone failure modes as possible sources of
interference. Furthermore, how will the Transportation Security
Administration and the crew be able to distinguish between a cell
phone and a jamming device? While jamming can be currently achieved
by other means, such as hiding a jamming device in a computer,
microelectronic technology has improved to spoof navigation systems
into telling a crew a wrong location. This may be an invitation to
terrorists to bring jamming equipment on an aircraft. I used to
work on the Future Combat System, and I know it's no secret that the
U.S. military is developing this technology in small packages. GPS
jamming technology is particularly well-developed. I remember one
incident where a jamming device spoofed an M1A1 Abrams crew into
believing they were somewhere where they were really not. If you do
that to an A380 crew, you could lose 800 people or even start a war.

The industry needs more time to work with the RTCA and the FAA to
develop solutions. Solutions are at least two years out. I would

want to bring in more people from the System Safety Society as well as the Society of Automotive Engineers before I rush to judgment. Furthermore, as a pilot, I would oppose the use right now unless I could interrupt a cell phone conversation to make an announcement. Now that would be a technical achievement. I want my passengers to know exactly what they need ot be doing when I speak. Seat belt use is at an all-time high I understand. Let's keep up the good work and help the FAA help pilots to keep passengers informed. Cell phones can impede this information.

These challenges before us can be met, but we are not ready for them. Patience is a virtue here that can save lives. So, my advice to the FCC is to wait until further notice from a broad consensus of those of us in the know. I look forward to working with you.

Respectfully,

David J. Sullivan-Nightengale

1132 Norton Street
Saint Paul, MN 55117

Home: (651) 489-1225
Cell: (651) 247-6410

e-mail: nigh0017@umn.edu

David J. Sullivan-Nightengale is a 1998 graduate of the United States Military Academy at West Point Class with a field of study of electrical engineering. Although he is a disabled veteran, he is also a private pilot and radio enthusiast. He served briefly as a Signal Corps platoon leader for two months while a cadet. He is a Profesional Member of the System Safety Society and is currently on medical leave from Honeywell due to combat related injuries. He has completed some graduate study in Computer Science, and will be attending the Master of Aeronautical Science program at Embry Riddle Aeronautical University with a focus on Aerospace Safety.